Net-Centric Enterprise Services (NCES)
User Guide

Version 1.3.2

1 September 2009

DISA

Revision History

Date	Version	Description
29 Jul 2005	0.1	Initial Draft
15 Aug 2005	0.2	Draft
25 Aug 2005	0.3	Draft
1 Sep 2005	0.4	Draft
8-13 Sep 2005	0.5	Added the necessary "install security SDK" to the beginning of all of the "consumer" workflows – added Section 1.4 – Rules of Engagement
19-20 Sep 2006	0.6	Corrections to workflows to point to new document workspace. Fixes for comments from NCES PMO.
26 Sep – 6 Oct 2006	0.7	Corrections to workflows based on developer inputs, NCES Division review, and corrections from "Dry Run" of NCES Support capabilities on 21-23 Sep 05.
21 Nov 2006	0.8	Updates to document to capture DOL Portal modifications and miscellaneous corrections.
17 Jan 2006	1.0	Corrections to non-working links. Clarified workflow instructions. Combined NIPR and SIPR guides. Added new references to the PKI User Guides.
20 Jul 2006	1.0	Added links to PKI Guides. Updated Service Discovery/ Service Provider Workflow. Updated End User section to reflect new Service Discovery portlet. New information on User/Pass for SIPR. Removed "draft". Removed references to Pilot WG. Updated date/version. Added information on new Collaboration service. Changed all references from ECB 1.1 to ECB 1.2.
7 Sep 2006	1.0	Replaced figure 2-4 and 2-9 with updated screenshots from the updated website and finalized formatting of the entire paper.
20 Apr 2007	1.1	Fixed Hyperlinks in various sections, revised MDR section to reflect upgrade from 5.1 to 6.0, updated help desk (now the GISMC) references and contact information, and added mention of DKO migration and the location of the "NCES Developer's Portal" in the document
12 Mar 2008	1.2	Update to reflect migration to DKO. Removed DOL related access information. Added DKO access information. Added NCES Developer Community information. Added notices to any references still pointing to DOL, or to functionality not yet available via DKO.

31 July 2009	1.3	Updated to reflect changes made since IOT&E.
20 August 2009	1.3.1	Revised to incorporate changes resulting form NCES PMO reviews (NE_B9, NE_B5, NE_B2, NE_A1)
1 September 2009	1.3.2	Updated to reflect changes made from NE_B6

Table of Contents

Table of Figures

Welcome to the Net-Centric Enterprise Services Program

Welcome to the Net-Centric Enterprise Services (NCES) Program. This program represents a critical part of our efforts to develop a set of workable Core Enterprise Services to support net-centricity throughout the Department of Defense (DoD). The NCES Program Status can be found at https://www.intelink.gov/wiki/Net-Centric_Enterprise_Services and https://www.intelink.gov/blogs/_nces/

NCES is making available the following capabilities on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet):

- User Access (Portal)
- Collaboration Service
- Service Security
- Mediation
- Content Discovery
- Content Delivery
- People Discovery
- Service Discovery
- Machine-to-Machine Messaging
- Metadata Discovery
- Enterprise Service Management (ESM)

This guide introduces end users and software developers to the services available within NCES program. The Web sites referred to in the guide provide detailed user support and technical information to facilitate service usage. Technical support access and availability also are discussed in the guide.

If you have comments or questions, please contact us at nces@csd.disa.mil or ncescolumbus@nocc.disa.smil.mil.

Once again, we are pleased to welcome you to the NCES Program and look forward to working with you and supporting your efforts to become more 'Net-Centric'.

How to Use This Guide

This guide provides information on how organizations can get involved within NCES. Participation gives end users and software developers an early opportunity to test the capabilities of the services and provide feedback to the NCES Program Management Office (PMO) for future updates to these services.

This guide explains the cycle of activities, or workflows, necessary for participants to learn more about the NCES Program, acquire documentation, and use NCES services. The guide also provides the workflows necessary for engaging Web service developers and helping them find instructions and tools for building interoperable services.

The guide provides several links to NCES Defense Knowledge Online (DKO) sites, such as the NCES Developer Community, Working-Level Integrated Product Team (WIPT) sites supporting NCES program management, and Working Group (WG) sites supporting NCES services development. Users must obtain access to the DKO to view these sites.

How This Guide Is Organized

- Section 1 presents general information on the NCES Program and how to get involved with NCES.
- Section 2 presents the steps users must follow to gain access to the NCES services and relevant documentation.
- Sections 3 through 6 describe how NCES users (end users, service consumers, service providers, and data providers) can use and integrate within the services.
- Section 7 contains PEO-GES contact information.

1 Introduction

Information on the Net-Centric Enterprise Services (NCES) Program is located at http://www.disa.mil/nces (NIPRNet) and http://www.disa.smil.mil/nces (SIPRNet).

1.1 Program Overview

The NCES Program is based on an emerging concept within DoD, called "net-centricity," which enables systems to provide the right information, to the right people, at the right time.

NCES supports new capabilities in the NIPRNet and SIPRNet DoD domains, bringing together Internet technology and the power of DoD. NCES enables the creation of a marketplace of information sources and services for DoD information. The program represents a different approach for DoD - an approach that is market-based, enterprise-wide and joint by design. NCES customers include the Warfighter, Intelligence, and Business domains - anyone within the DoD community who needs to share and retrieve information.

The NCES Increment One IOC was declared on June 8, 2009 which included Enterprise Collaboration, Content Delivery (GIG Content Delivery Service and Enterprise File Delivery), Metadata Discovery and User Access. The first Fielding Decisions (FD) currently scheduled for October 2009 will include Service Discovery. The second FD scheduled for March 2010 will consist of Content Discovery (Enterprise Search and Enterprise Catalog), Service Security, Mediation, ESM, Messaging, and People Discovery.

The NCES Program provides four product lines:

1. **Enterprise Service-Oriented Architecture (SOA) Foundation:** Enables DoD transformation by providing the core infrastructure that supports data and application interoperability, assessment of service, and data utilization. The core infrastructure reduces the complexity of DoD's information technology environment and promotes the reuse of existing information technology capabilities.

2. **Collaboration:** Provides collaboration services, such as whiteboard sessions, conferencing sessions, and instant messaging (IM), as well as DCO collaboration tools.

3. **Content Discovery & Delivery:** Supports efficient information advertisement, discovery, and delivery.

4**. User Access (Portal):** Provides a personalized, user-defined, web-based presentation and offers secure access to enterprise services and NCES toolkits. .DKO will provide the primary access point for user-facing services provided by NCES.

Each product line represents a bundled set of related capabilities that can be leveraged throughout the DoD Global Information Grid (GIG), thus negating the need for multiple DoD Programs of Record (POR) or Communities of Interest (COI) to build redundant functionality.

1.2 NCES Involvement

Members of the DoD community can become involved with the NCES Program in several ways.

- By becoming a user:

  Users are DoD end users and developers who support DoD Programs of Record or Communities of Interest and can access and use NCES services.

  Note: Developers can be government entities or commercial entities as long as commercial entities directly support a government program.

  Users can engage with NCES in one or more of the following ways:

  As an **End User:**
  End users can directly access some services via a portal environment. Services available to end users include Portal, Collaboration, People Discovery White Pages, Content Discovery and Delivery.

  As a **Service Consumer:**
  Service consumers are developers (government or commercial) that support DoD and have applications that use/interface with the services provided by NCES or by other Service Providers.

  As a **Service Provider:**
  Service providers are developers (government or commercial) that support DoD and have applications that provide their own services to the enterprise.

  As a **Data Provider:**
  Data providers are developers (government or commercial) that support DoD and have data to expose to the enterprise.

- By attending **Working-Level Integrated Product Team (WIPT)/Working Group (WG) Meetings**:

NCES has established WIPTs and lower-level WGs, chaired by NCES and/or ASD (NII) staff, to engage DoD stakeholders and users. A primary activity of WIPTs and WGs is the review of key acquisition activities and documents.

WIPTs and WGs meet regularly. Meeting dates and locations, and other information on WIPTs, are posted on the WIPT sites within DKO. Attendance is open to representatives of DoD organizations interested in becoming involved in the NCES Program.

NCES manages or leverages the following WIPTs and WGs. Because of the sensitive information that appears on some of these sites, separate registration may be necessary. Please contact the NCES PEO to join a WIPT or WG and obtain access to WIPT sites within DKO. The PEO email address is Contact_PEOGES@disa.mil.

- **NCES Test & Evaluation WIPT** (https://www.us.army.mil/suite/page/468920)
- **NCES Engineering WIPT** (https://www.us.army.mil/suite/page/465318)

1.3 Rules of Engagement

Users must provide the information discussed in this subsection to the GIG Infrastructure Services Management Center (GISMC). Section 7 of this document contains GISMC contact information.

Note: If a user falls into more than one category (listed below), he or she only needs to send a single email to the GISMC that contains the information required for all his or her applicable categories.

1.3.1 End Users

Do not need to provide any information to the GISMC.

1.3.2 Service Consumers

The organizational representative of a service consumer must provide the following information on the consuming system:

- Mission Assurance Category (MAC), Confidentiality Level (CL), and highest level of data classification (Definitions for MAC and CL are provided in Appendix B.)
- DoD Public Key Infrastructure (PKI) Server Certificate information
- Proof of Authority to Operate (ATO) and Authority to Connect (ATC) with the signature of the system's Designated Approval Authority (DAA)
- Organization's desired outcome of the partnership
- Resources (human and machine) needed from NCES
- Expected number of total and concurrent users accessing NCES
- Time frame for engagement and expected duration
- Performance and reliability requirements

- Machine and domain names

1.3.3 Service Providers

The organizational representative of a service provider must provide the following information on the system:

- MAC, CL, and highest level of data classification
- DoD PKI Server Certificate information
- Proof of ATO and ATC with the signature of the system's DAA
- Web Services Description Language (WSDL) document for registration in the NCES Service Discovery Service
- Organization's desired outcome of the partnership
- Resources (human and machine) needed from NCES
- Expected number of total and concurrent users accessing NCES
- Time frame for engagement and expected duration
- Performance and reliability requirements
- Machine and domain names

1.3.4 Data Providers

The organizational representative of a data provider must provide the following information on the system:

- Classification level of provided data
- DoD PKI Server Certificate information
- Proof of ATO and ATC with the signature of the system's DAA
- Organization's desired outcome of the partnership
- Resources (human and machine) needed from NCES
- Expected number of total and concurrent users accessing NCES
- Time frame for engagement and expected duration
- Performance and reliability requirements
- Machine and domain names

1.4 Glossary

A glossary of NCES Program terms and acronyms is available at http://www.disa.mil/nces/about_nces/glossary.html (NIPRNet) and http://www.disa.smil.mil/nces/about_nces/glossary.html (SIPRNet). A list of acronyms used in this guide is provided in Appendix A.

2 NCES User Access Information

2.1 Defense Knowledge Online (DKO) Access and Registration

To access NCES services and NCES information resources via the DKO portal, users must have or obtain a DKO account. To login or register for an account, start by accessing the portal at https://www.us.army.mil.

Note: The following portal images change periodically and are shown here for reference.

Figure 1: Assessing Portal

Click on "I Accept" (See Figure 1) to proceed to the Registration/Login Page (See Figure 2).

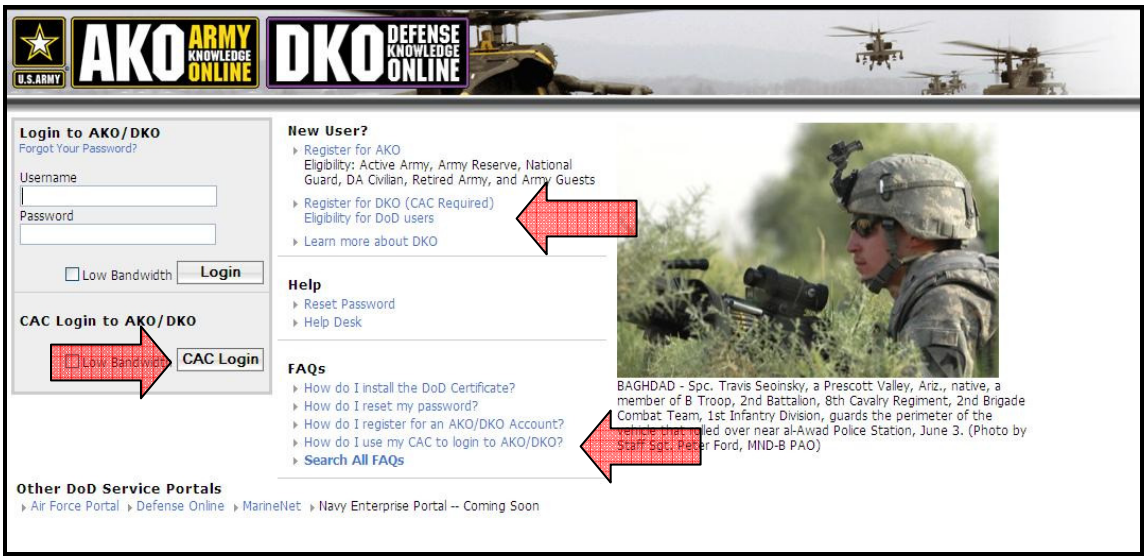

Figure 2: Login Page

If you have an account and have registered your Common Access Card (CAC), click on "**CAC Login**" to proceed (See Figure 2).

If you have an account and have not registered your Common Access Card (CAC), click on "**How do I use my CAC to login to AKO/DKO?**" (See Figure 2).

If you do not have a DKO account, click on "Register for DKO (CAC Required)" or "**How do I register for an AKO/DKO Account?**" for detailed instructions (See Figure 2).

After selecting **Register for DKO**, there will be several options for account types: Army Account, Joint Account, and Sponsored Account. Choose that account type appropriate for your situation and follow the instructions on the site. Active Army, Army Reserve, National Guard, DA Civilians, Retired Army, and Army Guests are eligible for Army Accounts.

2.2 Public Key Infrastructure Certificates

Nearly all NCES services require the use of PKI certificates for access. For individual end users of the services, this can mean a Common Access Card (CAC) or DoD issued software token certificate for NIPRNet, SIPRNet users need to obtain PKI Soft Certificates. Further, service consumers and service providers will need to obtain server certificates in order to interoperate with machine-to-machine services.

For more information on obtaining certificates, please see these guides (requires DKO access);

- End User:
  - "NCES PKI User's Guide for NIPRNET/Internet Use" https://www.us.army.mil/suite/doc/7434326
  - "NCES PKI User's Guide for SIPRNET Use" https://www.us.army.mil/suite/doc/7000038
- Service Consumer or Service Provider:
  - "NCES PKI System Administrators and Application Owners Guide for NIPRNET/Internet Use" https://www.us.army.mil/suite/doc/6999949
  - "NCES PKI System Administrators and Application Owners Guide for SIPRNET Use" https://www.us.army.mil/suite/doc/6999950

2.3 **Accessing the NCES Services** via DKO

The **DKO Home** page is the starting point for accessing the NCES services via DKO (services can be also be accessed via direct links and other DoD portals and web pages). New users may see the **AKO Home** page until they set their user preferences to display DKO as their Home page. If the **AKO Home** page is displayed, simply click on the "**Home**" drop down menu and select "**DKO Home**" (See Figure 3) to view the **DKO Home** page (Figure 4).

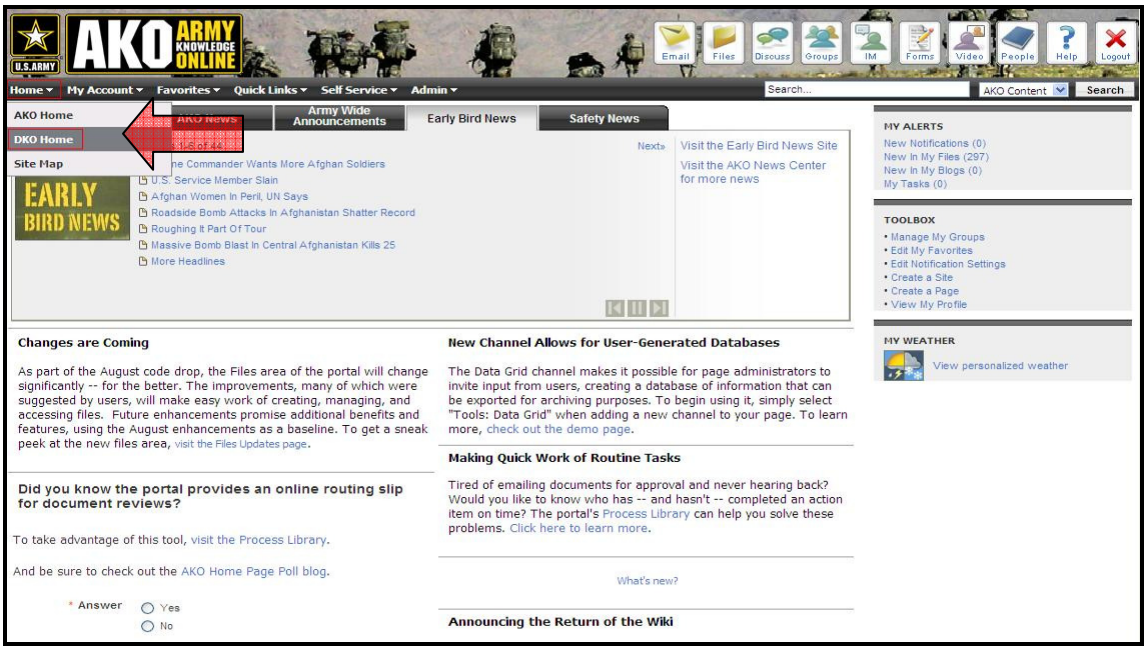

Figure 3: Navigate to DKO

On the **DKO Home** page (Figure 4), there is a section dedicated to accessing **NCES User Services** or NCES informational resources such as the **NCES Developer Community** portal, which is the portal for developers of **NCES Service Consumers**, **NCES Service Providers**, and **NCES Data providers** (See Figure 5).

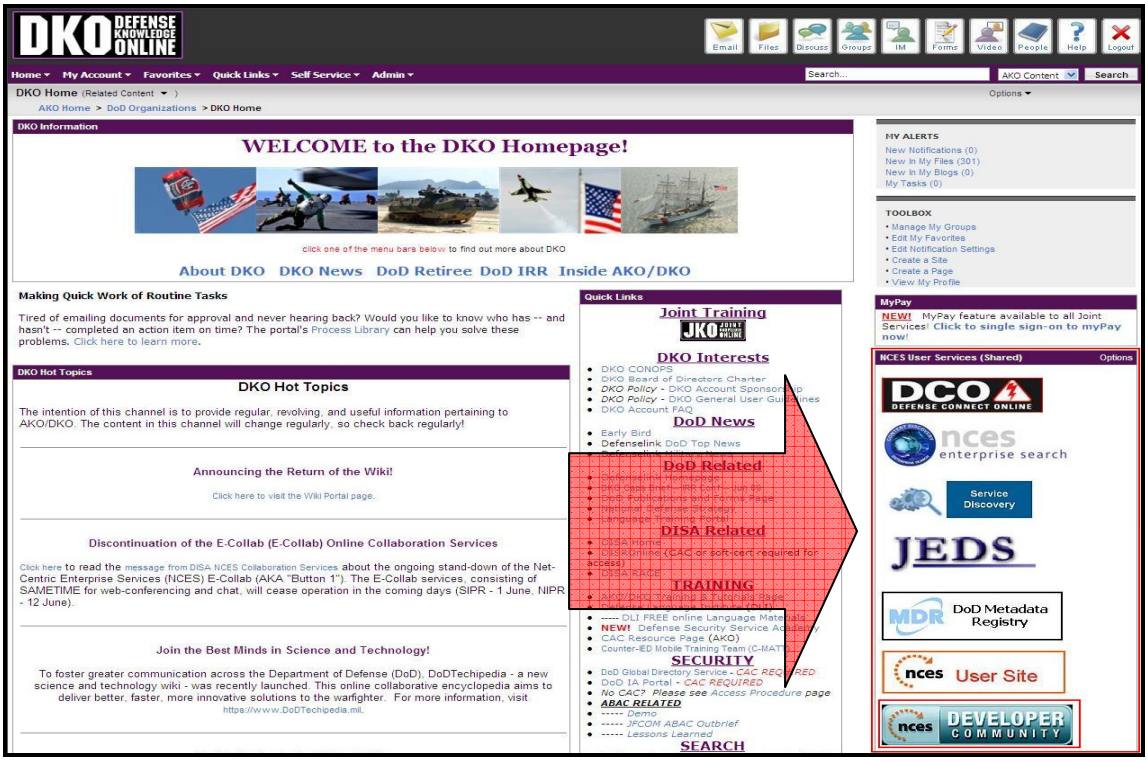

Figure 4 DKO Home Page

2.4 NCES Developer Community

The NCES Developer Community is the central location for finding documentation, resources, tools to support developers involved in creating net-centric services. The site contains developer guide pages, links to key external sites and documents, how-to guides for implementing the Net-Centric Data Strategy, developer information for each NCES service, developer forums, and other developer centric information (see Figure 5).

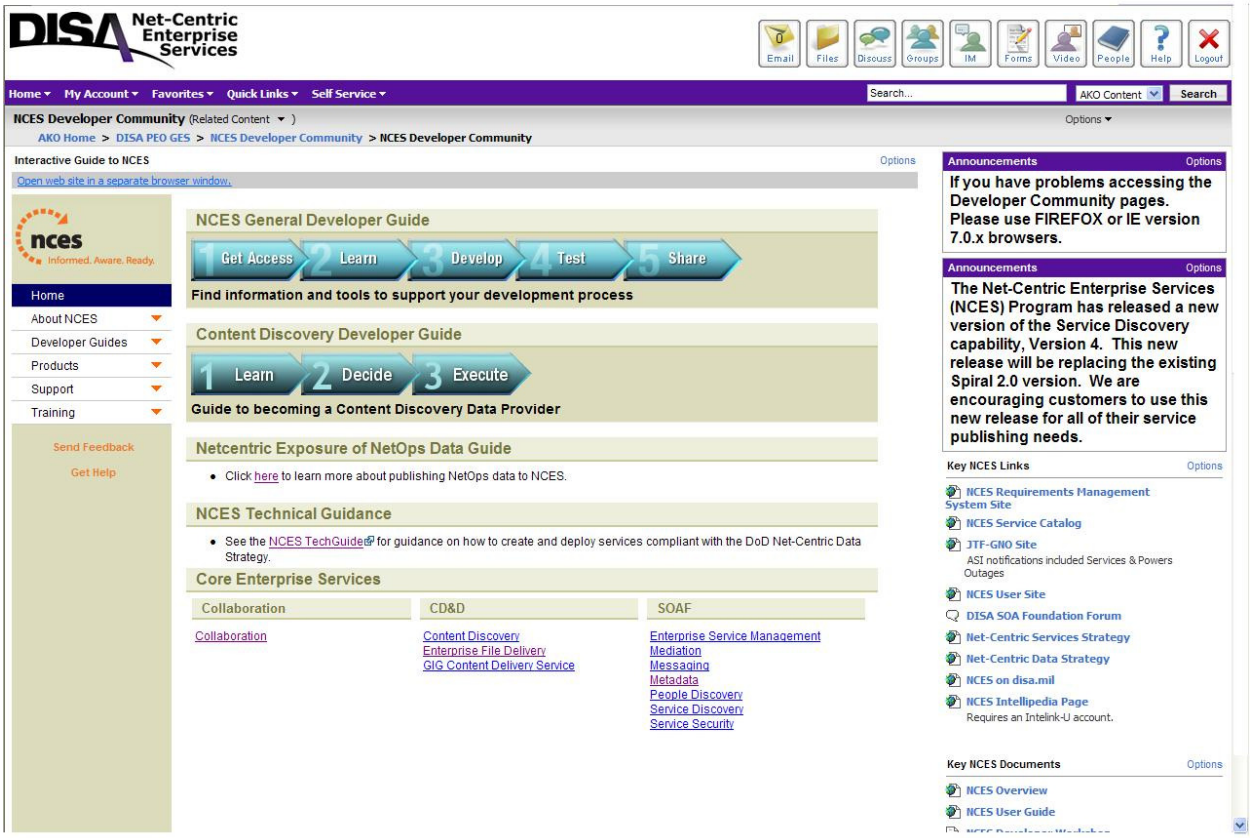

Figure 5: Developer Community Page

3 End User

As an end user, you can directly access certain NCES services, including the following:

- User Access (Portal)
- Collaboration
- Enterprise Search
- People Discovery White Pages
- Messaging
- Service Discovery

3.1 User Access (Portal)

The DKO is the DoD Enterprise Portal https://www.us.army.mil/suite/page/382109 [NIPRNet] or https://www.us.army.smil.mil/suite/page/5370 [SIPRNet]. It provides a personalized, user-defined, web-based presentation that enables secure access to various enterprise services (including information retrieval and posting), knowledge management, collaboration tools, and working groups.

3.1.1 Search

From any page, you can perform simple searches for people or information by using the search bar at the top right.

3.1.2 Sites and Folders

You may create your own site with a folder to enable you to collaborate with other portal users by using the Create Site function on the My Workspace page. Total file storage is restricted to 50 megabytes per user. DoD organizations may request creation of organizational sites, which have unlimited space. You may access other sites under Site Map or by searching for sites using the Search function.

3.1.3 Training

AKO, as the infrastructure provider for DKO, provides numerous online training guides, as well as classroom style training opportunities. The starting point for learning about the portal at https://www.us.army.mil/suite/page/139150 .

3.2 Collaboration

The NCES Collaboration service enables synchronous and asynchronous communication using instant messaging, low-bandwidth text chat, and web conferencing. Instant messaging and web conferencing both include text-based communication, while web conferencing adds shared whiteboards, desktop & application sharing, and the ability to invite non-DoD personnel into collaboration sessions.

There is an instance of the Collaboration service Defense Connect Online (DCO). Users are free to use this service.

Access DCO Collaboration at (https://connect.dco.dod.mil/). A valid CAC PKI certificate is required for access for NIPRNet or User ID and Password to log in.

3.3 Enterprise Search

The Enterprise Search capability is a web-based search application that includes content crawled by the centralized search engine, search results from federated search sources, and Enterprise Catalog results. The Centralized Search service crawls and indexes content on web sites. Examples of content providers who would utilize centralized search would be those whose content may be discovered by anonymous or authenticated users with access to the network. Those whose content contains text or text metadata, such as HTML, plain text, Word documents, PowerPoint, and PDFs. The Federated Search service allows users to discover information from disparate data sources with one query, accessing multiple repositories and websites. It provides a search service that receives queries from users and applications and federates them to the NCES enterprise catalog and across the enterprise to user-selected data sources enabled with the federated search interface. The federated search service supports aggregation and elimination of duplicate results from remote data sources and preserves access controls implemented at the data source. Examples of content providers who would utilize the federated search service would be those with large repositories, security constraints or dynamic content. Commercial plug-ins are available for many commercial applications allowing for simple integration with the federated search service.

3.4 People Discovery White Pages

People Discovery provides services to publish and find information on GIG users and connected devices. User information is provided by the Mission Assurance Program Executive Office (PEO-MA) Joint Enterprise Directory Services (JEDS), which aggregates a number of DoD repositories of user information. This capability is currently available only on the NIPRNet. A White Pages application is available to search for users. The White Pages are linked within DKO or are accessible directly at https://jeds.gds.disa.mil/ . A valid DoD PKI certificate or ECA certificate is required for access.

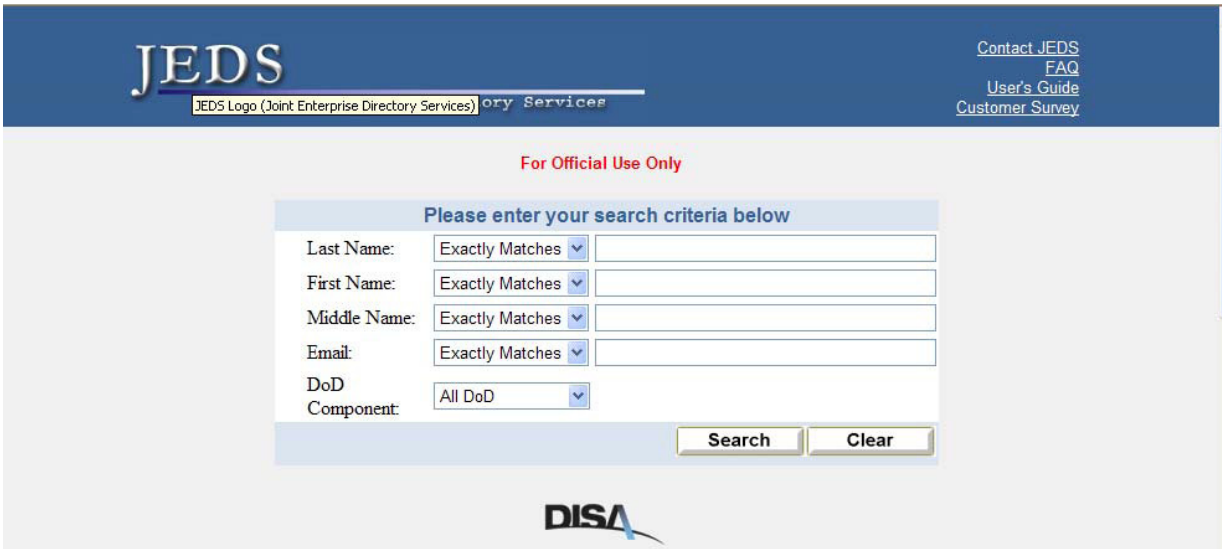

Figure 6: White Pages Interface

Note: The White Pages Interface will be updated to reflect the new version JEDS 2.0 soon.

3.5 Service Discovery

Service Discovery provides technical information about Web services and is typically not a capability that is used by the End User

4 Service Consumer

This section provides information for users who participate in the NCES Program as service consumers. To participate in the program, you must first register as described in Section 1.3.2.

Note: For SIPRNet users, you must be registered as a user on DKO-S and MDR-S in order to access the SIPR UDDI registry.

4.1 Security Enable Your Consuming Application

If your application will consume an enterprise service that implements the NCES Service Security specification, such as the Messaging or Federated Search services, it must format its SOAP requests to comply with the specification. The NCES Service Security SDK provides support for invoking such services. The following steps are for downloading and deploying a sample application that uses the Service Security Software Development Kit (SDK). These steps prepare you, as a service consumer, for developing applications using the Service Security SDK.

Note: The SDK has been deprecated by NCES, which will not maintain the software in the future. The SDK will be released as part of an open source Government Off-The-Shelf (GOTS) security solution.

Step 1. Open the NCES Developer Community Site on DKO

Go to https://www.us.army.mil/suite/page/384284

Step 2. Navigate to Products > SOAF

Step 3. Select Service Security
This page contains extensive information on Service Security and
The Links section contains a link to the NCES Service Security Spiral 1.1, which includes an SDK (including Java and .Net SDKs), the NCES Service Security SDK User's Guide, the Data Gathering Checklist, and other documents.

4.2 Consuming or Integrating with SOA Foundation Services

This section describes how you, as a service consumer, can consume or integrate with SOA Foundation Services.

4.2.1 Mediation Service

The NCES Mediation Service provides the ability to expose existing POR data transformation and protocol adaptation mediation capabilities by leveraging the NCES Metadata Registry, Service Discovery, and Enterprise Catalog search capabilities. The capability is oriented to software developers who are interested in identifying mediation capabilities that they may be able to reuse.

The following steps will guide you to the Mediation page on the NCES Developer Community site for the latest information.

Step 1. Open the NCES Developer Community Site on DKO
Go to https://www.us.army.mil/suite/page/384284

Step 2. Navigate to Products > SOAF

Step 3. Select Mediation
This page contains the latest information on the Mediation capability.

4.2.2 Messaging

This section describes the steps for using the Messaging capabilities.

Step 1. Open the NCES Developer Community Site on DKO
Go to https://www.us.army.mil/suite/page/384284

Step 2. Navigate to Products > SOAF

Step 3. Select Messaging
The "Downloads" section contains the Messaging SDK.

Step 4. Download Package

The Messaging SDK package contains documentation about the NCES Messaging service and a set of sample applications demonstrating its functionality. The documentation includes an overview of the Messaging service, a developer's guide that discusses technical details (such as the service specifications used), and a guide to the Messaging SDK that provides details on the sample applications. The sample applications, which exercise the functionality of the Messaging service, are already integrated with NCES service security and only require a valid certificate and configuration of the proper roles for the certificate's domain name.

Step 5. Install Messaging SDK
Unzip the Messaging SDK in a directory on the host machine. The sample applications are written in Java and will run on most operating systems. For convenience, a set of Microsoft Windows batch scripts is provided for running the various applications.

Step 6. Deploy Sample Application
The sample applications may be used to publish messages and subscribe to message channels. The applications enable developers to understand the operation of the Messaging service before integration into new applications.

Step 7. Test Sample Application
You may use the sample applications to test the configuration of the Messaging SDK. A valid PKI certificate must be obtained and installed for the applications to operate correctly. In addition, the NCES identity store must be configured with the proper roles for the certificate's domain name. Testing these configurations using the sample applications provides a controlled means to test your environment.

Step 8. Integrate Messaging SDK with Consuming Application
The Messaging SDK provides source code for the sample applications. The sample applications provide examples for the development of new consumer applications or the integration of messaging functionality into existing consumer applications.

4.2.3 Service Discovery

Service Discovery provides technical information about Web services that are available within the DoD enterprise. Service Providers, who are responsible for implementing, supporting and managing these Web services, use Service Discovery to register, or publishing information about their specific services in a service registry. Service Consumers use Service Discovery to search for and find information about available Web services.

The Service Discovery capability provides a query interface for Service Consumers, which allows them to search for and find services and service information. Service Consumers can then determine, based on the published information, if a service is appropriate for their use.

The Service Discovery user interface is available from the DoD Metadata Registry (MDR) interface, as shown in Figure 7, and can be accessed by anyone with an AKO/DKO account and an MDR account (on NIPRNet). To access this service, using single sign-on (SSN), the user should log into DKO (https://www.us.army.mil/suite/page/382109) NIPRNet, access the MDR

using the appropriate link from the DKO Homepage and then link to the NCES Service Discovery user interface using the appropriate link on the MDR Home page.

Appropriate User Manuals and CONOPS are also available from this user interface.

Service Discovery is also available on SIPRNet, via DKO-S and MDR-S.

Figure 7: NCES Service Discovery

The Service Discovery interface provides two basic search capabilities, one to search for Service Providers and one to search Services. The following figure (Figure 8), is an example of the Category search capability of the Service Discovery user interface.

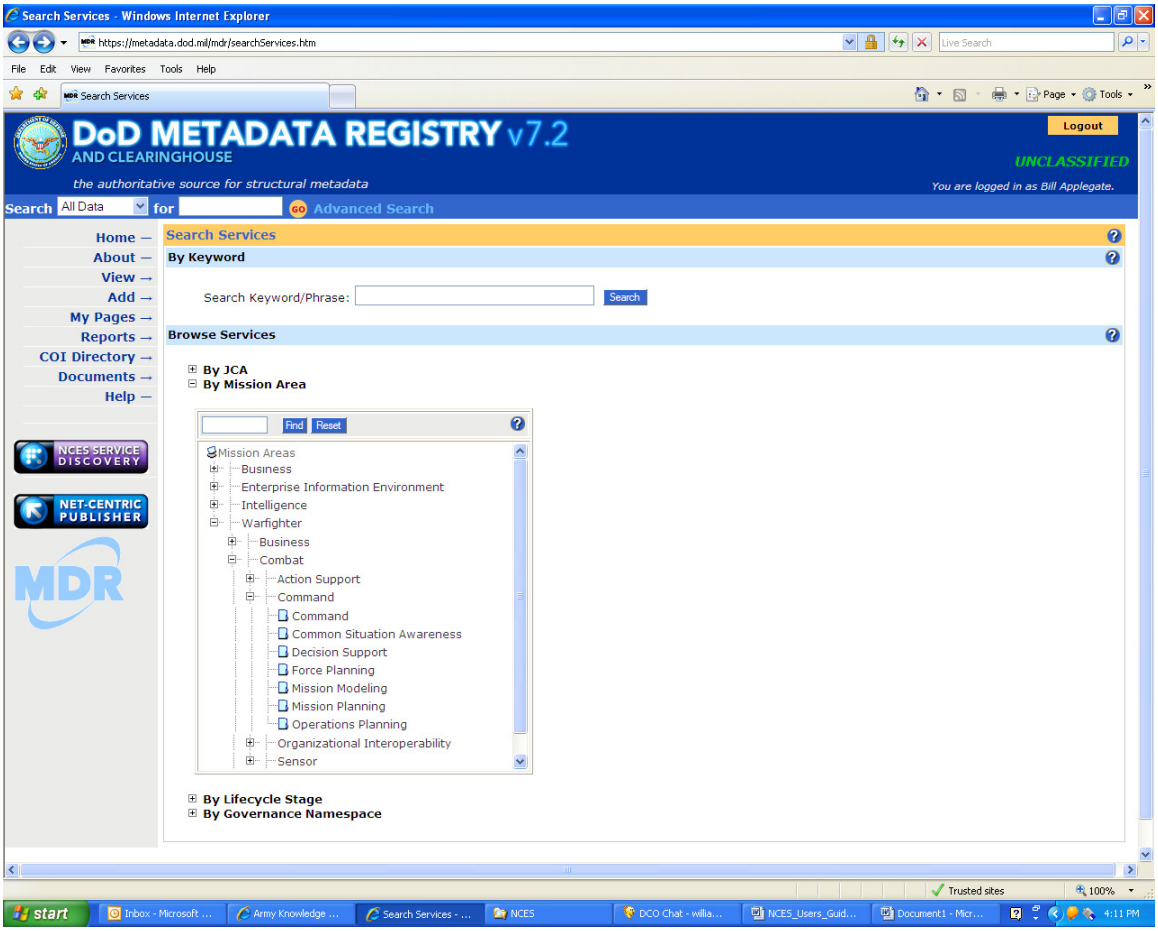

Figure 8: Category Search

A Service Consumer may also use the UDDI Inquiry API to access the UDDI Registry directly. This allows the Service Consumer to access service information at runtime, using a web service interface. Use of this Inquiry web service interface requires a valid DoD PKI Certificate. This interface is fully documented in the NCES Service Discovery Web Services Manual https://www.us.army.mil/suite/doc/16306814 that can be downloaded from the Service Discovery page on the NCES Developer Community Site on DKO.

4.3 Consuming or Integrating with NCES Content Discovery Services

This section describes how you, as a service consumer, can consume or integrate with NCES Content Discovery services.

4.3.1 Enterprise Search

The section describes the steps for using the Enterprise Search capabilities of NCES services.

Step 1. Open the NCES Developer Community Site on DKO

Go to https://www.us.army.mil/suite/page/384284

Step 2. Navigate to Products > CD&D

Step 3. Select Content Discovery
The **Downloads** section contains the Content Discovery SDK.

Step 4. Download Package
The package contains documentation and sample applications for the NCES Content Discovery services, which includes both the NCES Federated Search and NCES Enterprise Catalog services. The documentation consists of an overview of the NCES Content Discovery services, a developer's guide that discusses the details of the service specifications, and an SDK guide that discusses installation and utilization of the sample applications in the SDK.

Step 5. Unzip the Content Discovery Service SDK
Unzip the SDK in a directory.

Step 6. Deploy Sample Application
The SDK documentation outlines how to configure and utilize the sample applications to access the NCES Content Discovery service.

Step 7. Test Sample Application
Once configured, you can use the sample NCES Content Discovery applications to submit queries to the enterprise. A successful test of the application demonstrates the correct configuration of the certificates and roles for NCES security services.

Step 8. Integrate Federated Search Service SDK with Consuming Application
The sample applications provide source code, which enables you to develop new applications or integrate Content Discovery capabilities into existing applications.

4.3.2 Enterprise Catalog

This section describes the steps for using the Enterprise Catalog service.

Step 1. Open the NCES Developer Community Site on DKO
Go to https://www.us.army.mil/suite/page/384284

Step 2. Navigate to Products > CD&D

Step 3. Select Content Discovery
The **Downloads** section contains the Content Discovery SDK.

Step 4. Download Package
The package contains documentation and sample applications for the NCES Content Discovery services, which includes both the NCES Federated Search and NCES Enterprise Catalog services. The documentation consists of an overview of the NCES Content Discovery services, a developer's guide that discusses the details of the service specifications, and an SDK guide that discusses installation and utilization of the sample applications in the SDK.

Step 5. Unzip the Content Discovery Service SDK
The SDK may be unzipped in a directory.

Step 6. Deploy Sample Application
The SDK documentation outlines how to configure and utilize the sample applications to access the NCES Content Discovery service.

Step 7. Test Sample Application
Once configured, the Service Consumer can use the sample NCES Content Discovery applications to submit queries to the enterprise. A successful test of the application demonstrates the correct configuration of the certificates and roles for the NCES security services.

Step 8. Integrate Enterprise Catalog SDK with Consuming Application
The sample applications provide source code, which allows the Service Consumer to develop new applications or integrate Enterprise Catalog capabilities into existing applications.

4.4 Consuming Customer-Provided Services

Customer-provided services will be identified through Service Discovery and consumed via the WSDL-defined interface or the integration of Service Provider SDKs.

5 Service Provider

This section provides information for individuals who participate in the NCES Program as service providers. To participate in the program, you must first register as described in Section 1.3.3.

Note: For SIPRNet users, you must be registered as a user on DKO-S and MDR-S in order to access the SIPR UDDI registry.

5.1 Publish, Use, and Integrate with SOA Foundation Services

5.1.1 Service Discovery

Service Discovery provides technical information about Web services that are available within the DoD enterprise. Service Providers, who are responsible for implementing, supporting and managing these Web services, use Service Discovery to register, or publishing information about their specific services in a service registry. The NCES Program has integrated the service publishing capability of Service Discovery with the DoD Metadata Registry (MDR) and the Enterprise Catalog; enabling Service Providers to register service metadata in the MDR, and generate a DDMS record for Enterprise Search, at the same time as they register their services in the NCES Service Registry.

The Net-Centric Publisher (NCP) is the publishing interface for Service Discovery, which is available from the DoD Metadata Registry (MDR) interface, as shown in Figure 9, and can be accessed by anyone with an AKO/DKO account and an MDR account (on NIPRNet). To access this service, using single sign-on (SSN), the user should log into DKO

(https://www.us.army.mil/suite/page/382109) NIPRNet, access the MDR using the appropriate link from the DKO Homepage and then link to the Net-Centric Publisher user interface using the appropriate link on the MDR Home page.

Appropriate User Manuals and CONOPS are also available from this user interface.

The Net-Centric Publisher is also available on SIPRNet, via DKO-S and MDR-S.

Figure 9: Net-Centric Publisher

The Net-Centric Publisher (see Figure 10) enables Service Providers to publish information about their services in the NCES Service Registry, publish metadata related to their services in the DoD Metadata Registry and create Enterprise Catalog DDMS records about their services using a single user interface.

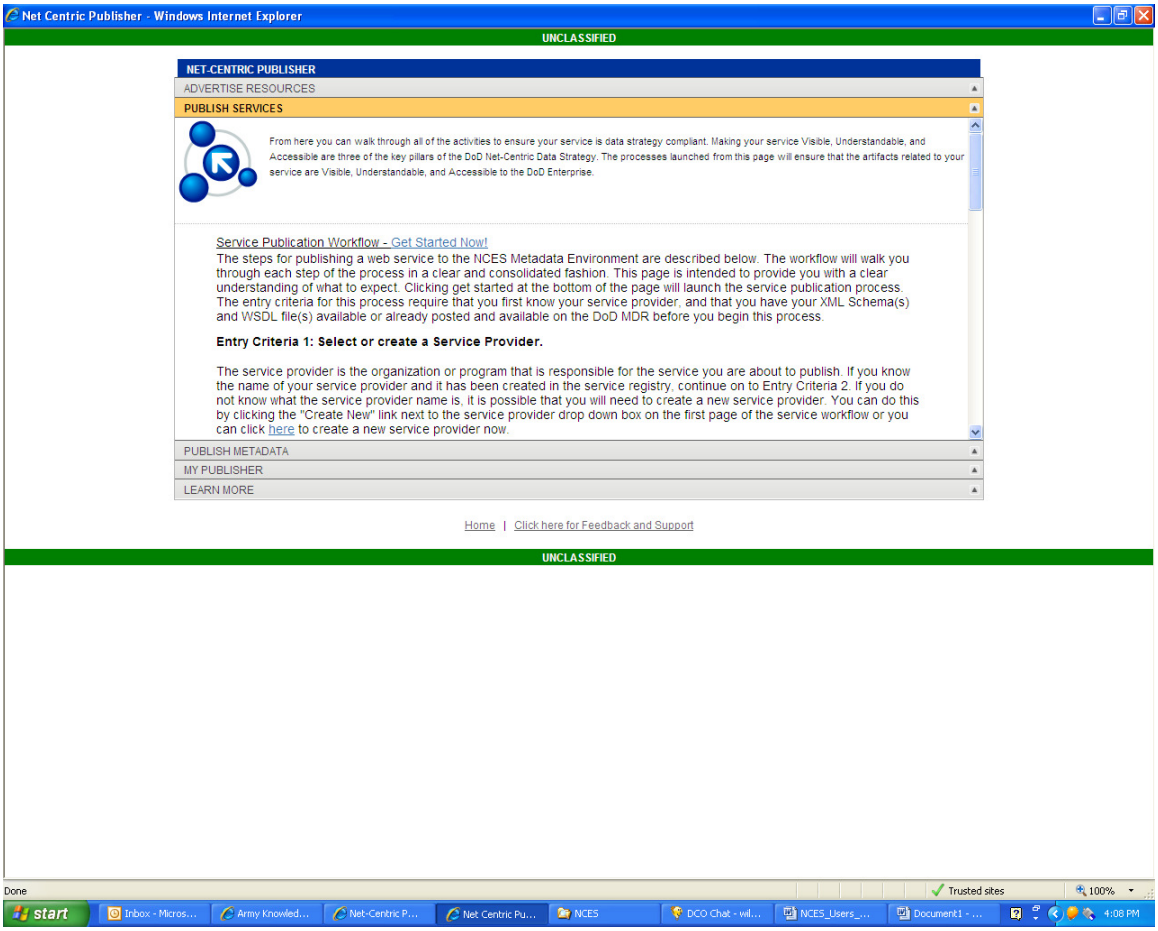

Figure 10: Service Publishing

A Service Provider may also use the UDDI Publication API to access the UDDI Registry directly. This allows the Service Provider to manage their own service information, using a web service interface. Use of this Publishing web service interface requires a valid DoD PKI Certificate and also requires a formal agreement with the NCES Program. This interface is fully documented in the NCES Service Discovery Web Services Manual (https://www.us.army.mil/suite/doc/16306814) that can be downloaded from the Service Discovery page on the NCES Developer Community Site on DKO.

6 Data Provider

This section provides information for individuals who participate in the NCES Program as data providers. To participate in the program, you must first register to become a Data Provider as described in Section 1.3.4.

Note: For SIPRNet users, you must be registered as a user on DKO-S in order to access the SIPR UDDI registry.

6.1.1 Publish Content Using NCES Content Discovery

The Enterprise Catalog service is capable of submitting and indexing DDMS metadata to data sources. As a data provider, you may visit the Department of Defense Discovery Metadata Specification Homepage for information on how to tag your content at (http://metadata.dod.mil/mdr/irs/DDMS/). The Enterprise Catalog Web service can be utilized through the Enterprise Client provided with the Content Discovery SDK. Download the Content Discovery SDK from the NCES Developer Community at https://www.us.army.mil/suite/page/384284.

6.1.2 Expose Content Using NCES Content Discovery

The Federated Search Web Service specification provides a standard query interface allowing NCES Content Discovery Services to submit a query to a data provider. As a data provider, you may execute the query, which returns the results containing DDMS-compliant metadata. The results are then aggregated with results returned from other data providers and returned to the user through end-user applications. Sample implementations of a data provider for the Federated Search Web Service will be added to the Content Discovery SDK. The Content Discovery SDK can be downloaded from the NCES Developer Community at https://www.us.army.mil/suite/page/384284

6.2 DoD Metadata Registry Information

The DoD Metadata Registry enables you to publish metadata artifacts (e.g., schemas, stylesheets, and taxonomies) to a portal available to the DoD community. Making user metadata products visible to the community enables others to reuse the user's hard work and promotes interoperability between systems. To use the services provided, the user must be a registered user on the Metadata Registry Portal. The Metadata Registry Portal supports single sign-on with the DKO. Simply click on the Metadata Registry button from the DKO home page. Otherwise, to register as a user on the Metadata Registry Portal, follow the instructions at https://metadata.dod.mil/mdr/register.htm (NIPRNet) or https://metadata.dod.smil.mil/mdr/register.htm (SIPRNet). The account created will provide access to the data within the portal and the ability to register new data products. The account also will provide access to the runtime APIs for application access to the metadata products.

Metadata products are registered in the Metadata Registry by creating a submission package and submitting the package file. Details on building a submission package, using package creation tools, validating the package, and submitting a package are available at https://metadata.dod.mil/mdr/downloads/manuals/MDR-services.zip (NIPRNet) or https://metadata.dod.smil.mil/mdr/downloads/manuals/MDR-services.zip (SIPRNet). Please note that the user must log in to view the referenced document. If a user encounters problems accessing the DoD Metadata Registry, he or she can submit questions or provide feedback at https://metadata.dod.mil/mdr/feedback.htm (NIPRNet) or https://metadata.dod.smil.mil/mdr/feedback.htm (SIPRNet). Registered users of the Metadata Registry can access the DoD Metadata Registry Portal at https://metadata.dod.mil.

The DoD Metadata Registry also provides Web Services access to locate XSL translations between XML schemas at runtime. Section 4.2.1 describes the workflow for discovering and

using a registered XSL translation. The WSDL for this service is available at https://metadata.dod.mil/mediation/MediationService?WSDL (NIPRNet) or https://metadata.dod.smil.mil/mediation/MediationService?WSDL (SIPRNet).

6.3 Developer Technical Guidance

The NCES TechGuide is the place to find out how to share information across the DoD and beyond using capabilities provided by the Net-Centric Enterprise Services (NCES) Program. NCES provides an infrastructure comprised of Core Enterprise Services (CES) to support the goals of the DoD Net-Centric Data Strategy. This site focuses on the technical and procedural information Developers, Architects and Program Managers need to create and deploy services which are visible, accessible and understandable to other GIG participants. It is available on the Metadata Registry Portal at https://metadata.dod.mil/mdr/ns/ces/techguide/, and is also linked from the NCES Developer Community.

7 For More Information

For general information about NCES, go to the following:

- NIPRNet https://www.us.army.mil/suite/page/483236 or https://www.disa.mil/nces
- SIPRNet: https://www.us.army.smil.mil/suite/page/5370 or http://www.disa.smil.mil/nces

For technical support, contact the NCES Technical Assistance Center, which operates 24 hours a day, 7 days a week. NCES users may contact the following:

Toll Free: 1-800-447-2457
Commercial: 614-692-3136
DSN: 850-3136
Unclassified Fax: 614-692-4040
Classified email: ncessupportteam@csd.disa.mil
Unclassified email: nces@csd.disa.mil
General Questions and Requests Email: Contact_PEOGES@disa.mil

DoD PKI Help Desk:

- (800) 490-1643, option 5 (toll free)
- Unclassified Email: weblog@chamb.disa.mil

Appendix A. Acronyms

AKO	Army Knowledge Online
API	Application Program Interface
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
ATC	Authority to Connect
ATO	Authority to Operate
CAC	Common Access Card
CD&D	Content Discovery and Delivery
CL	Confidentiality Level
COI	Community of Interest
DAA	Designated Approval Authority
DCO	Defense Connect Online
DDMS	Department of Defense Discovery Metadata Specification
DISA	Defense Information Systems Agency
DKO	Defense Knowledge Online
DoD	U.S. Department of Defense
DOL	Defense Online
DSN	Defense Switched Network
ECA	External Certificate Authority
ESM	Enterprise Service Management
EUT	Early User Test
GES	Global Information Grid Enterprise Services
GIG	Global Information Grid
GISMC	GIG Infrastructure Services Management Center
GOTS	Government Off-The-Shelf
IM	Instant Messaging
JEDS	Joint Enterprise Directory Services
JDK	Java Developer Kit
JKO	Joint Knowledge Online
LDAP	Lightweight Directory Access Protocol
M2M	Machine-to-Machine
MAC	Mission Assurance Category
MDR	Metadata Registry
NCES	Net-Centric Enterprise Services
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POR	Program of Record
QName	Qualified Name
QRG	Quick Reference Guide
RSS	Rich Site Summary
SDK	Software Development Kit
SIPRNet	Secret Internet Protocol Router Network
SOA	Service-Oriented Architecture
SOAF	Service-Oriented Architecture Foundation
SSO	Single Sign-On

UDDI	Universal Description Discovery and Integration
WG	Working Group
WIPT	Working-level Integrated Product Team
WSDL	Web Services Description Language
XML	eXtensible Markup Language
XSD	XML Schema Definition
XSL	eXtensible Stylesheet Language
XSLT	eXtensible Stylesheet Language Translation

Appendix B. Mission Assurance Categories and Confidentiality Levels

The following definitions of Mission Assurance Category (MAC) and Confidentiality Level (CL) are taken from DODI 8500.2.

Confidentiality Level. Applicable to U.S. Department of Defense (DoD) information systems, the confidentiality level (CL) is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). DoD has three CLs: classified, sensitive, and public.

Mission Assurance Category. Applicable to DoD information systems, the Mission Assurance Category (MAC) reflects the importance of information to the achievement of DoD goals and objectives, particularly the Warfighters' combat mission. MACs are primarily used to determine availability and integrity requirements. DoD has three MACs:

- **MAC I.** This category consists of systems that handle information that is vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

- **MAC II.** This category consists of systems that handle information that is important for supporting deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can be tolerated for a short time only. The consequences could include delay or degradation in providing important support services or commodities, which could seriously impact mission effectiveness and/or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure mission assurance.

- **MAC III.** This category consists of systems that handle information that is necessary for the conduct of day-to-day business but that does not materially affect support to deployed or contingency forces in the short term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

This page has been left blank intentionally.